UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,904	01/24/2002	Jeffrey D. Carr	1875.1310002	3811

26111	7590	09/29/2005

STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

(

	Application No.	Applicant(s)
Office Action Summary	10/053,904	CARR, JEFFREY D.
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-22_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-22_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _1/2/03_.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1- 22 are pending for examination.

2.   Claims 1- 22 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 19 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim recites a "method", where the dependency is on a system for claim 16. For the sake of applying art, the examiner assumes that "The system" is the correct phrase.

Claim 20 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim recites a "claim 13" dependency, where the dependency is on a system for claim 16. For the sake of applying art, the examiner assumes that "claim 16" is the correct phrase.

Claim 12 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim recites a "multilayer ..." algorithm, where the correct phrase for the

abbreviation MMH is "multilinear". For the sake of applying art, the examiner assumes that

"multilinear" is the correct phrase.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this
> or a foreign country, before the invention thereof by the applicant for a patent.

3.   Claims 1- 22 are rejected under 35 U.S.C. 102(a) as being anticipated by Ellington et al,

U.S. Patent 6,708,218 B1.

4.   As per claim 1; "A method of processing a packet having a plurality of layers,

comprising:

processing a first layer in accordance with a first protocol [ABSTRACT, col. 3,lines 1-

54, col. 4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the

determination of a frame as being IP frame or an IPSec frame via the MAC header and protocol

field in the IP header as examined in the data link control layer (i.e., col. 3,lines 17-54), clearly

encompasses the claimed limitations as broadly interpreted by the examiner]; and

processing a second layer in accordance with a second protocol in parallel with

processing of said first layer when processing of said first layers uncovers

sufficient information to support processing of said second layer

[ABSTRACT, col. 3,lines 1-54, col. 4,lines 25-col. 5,line 21, figures 3-11 and

associated descriptions, whereas the determination of a frame as being IP frame or

an IPSec frame via the MAC header and protocol field in the IP header (i.e., first

layer) as examined in the data link control (i.e., second) layer (i.e., col. 3,lines 17-

54), clearly encompasses the claimed limitations as broadly interpreted by the

examiner].".

5.   As per claim 2; "A method of processing a data packet according to a plurality of security

policies, comprising the steps of:

        (a) receiving the packet;

        (b) identifying a first security policy;

        (c) processing the packet according to

                the first security policy [ABSTRACT, col. 3,lines 1-54, col. 4,lines 25-col. 5,line

        21, figures 3-11 and associated descriptions, whereas the determination of a frame as

        being IP frame or an IPSec frame via the MAC header and protocol field in the IP header

        as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

        inherently uses Security association management (SA) and key exchange (i.e., first

        security policy), clearly encompasses the claimed limitations as broadly interpreted by

        the examiner];

        (d) identifying a second security policy when

                information necessary for said identification of the second security policy

        becomes available; and

        (e) processing the packet according to

the second security policy, concurrently with step (c) [ABSTRACT, col. 3,lines 1-54, col. 4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec inherently uses Security association management (SA) and key exchange (i.e., second security policy; layer dependent), clearly encompasses the claimed limitations as broadly interpreted by the examiner].".

As per claim 16, this claim is the apparatus/system for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection; "A system for processing a data packet according to a plurality of security policies, wherein processes that effect respective security policies can execute in parallel, the system comprising:

a packet identification (PID) parser that

identifies the packet;

a plurality of security processing modules, each of which can process the packet according to

one of the security policies in parallel with

at least one other security processing module; and

at least

one feedback loop or

feeding output of at least one of said security processing modules to

at least one other security processing module.".

6. As per claim 19; this claim is the intended use embodiment of claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection (A recitation directed to the manner in which a claimed apparatus is *intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform* (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references disclosing generally electrically equivalent embodiments such as that implemented using* Digital Video Broadcast (DVB) descrambler *hardware.)*; "The *method* of claim 16, wherein

said security processing modules comprise

a module for performing Digital Video Broadcast (DVB) descrambling.".

7. Claim 3 *additionally recites* the limitation that; "The method of claim 2, wherein

said step (c) comprises

decryption of data in the packet.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col. 4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec inherently uses Security association management (SA) and key exchange (i.e., first security policy) in support of the associated encryption/decryption cryptographic functions (i.e., col. 5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

8.   As per claim 6; this claim is the intended use embodiment of claim 3 above, and is

rejected for the same reasons provided for the claim 3 rejection (A recitation directed to the

manner in which a claimed apparatus is *intended to be used does not distinguish the claimed*

apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114

and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references*

disclosing generally algorithm/software implemented equivalent embodiments such as that

implemented using the ARC4 stream cipher encryption algorithm derivative of the associated

(RFC) 2401, "Security Architecture for the Internet Protocol" *standard of Ellington et al.)*; "The

method of claim 3, wherein

> said decryption is performed according to
>
>> the ARC4 algorithm.".

As per claim 10, this claim is the apparatus/system for the method claim 6 above, and is

rejected for the same reasons provided for the claim 6 rejection; "The method of claim 7,

wherein

> said decryption is performed according to
>
>> the ARC4 standard.".

9.   Claim 4 *additionally recites* the limitation that; "The method of claim 3, wherein

said decryption is performed according to

the data encryption standard (DES).".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated encryption/decryption cryptographic functions (i.e., col.

5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 17, this claim is the apparatus/system for the method claim 4 above, and is

rejected for the same reasons provided for the claim 4 rejection; "The system of claim 16,

wherein

said security processing modules comprise

a module for performing decryption according to the DES.".

10.   Claim 5 *additionally recites* the limitation that; "The method of claim 3, wherein

said decryption is performed according to

the triple data encryption standard (3DES).".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated encryption/decryption cryptographic functions (i.e., col.

5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 18, this claim is the apparatus/system for the method claim 5 above, and is

rejected for the same reasons provided for the claim 5 rejection; "The system of claim 16,

wherein

    said security processing modules comprise

        a module for performing decryption according to the 3DES.".

11.   Claim 7 *additionally recites* the limitation that; "The method of claim 2, wherein

    said step (e) comprises

        decryption of data in the packet.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated encryption/decryption cryptographic functions (i.e., col.

5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

12.   Claim 8 *additionally recites* the limitation that; "The method of claim 7, wherein

        said decryption is performed according to

            the DES.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated encryption/decryption cryptographic functions (i.e., col.

5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

13.   Claim 9 *additionally recites* the limitation that; "The method of claim 7, wherein

        said decryption is performed according to

the 3DES.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated encryption/decryption cryptographic functions (i.e., col.

5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

14.   Claim 11 *additionally recites* the limitation that; "The method of claim 2, wherein

        said step (e) comprises

            authentication of the data packet.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated authentication/encryption/decryption cryptographic functions

(i.e., col. 5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol", section

4.4.1 "The Security Policy Database", where the authentication/encryption/decryption

cryptographic functions include; AH use of SHA-1/HMAC), clearly encompasses the claimed

limitations as broadly interpreted by the examiner.).

15.   As per claim 12; this claim is the intended use embodiment of claim 11 above, and is

rejected for the same reasons provided for the claim 11 rejection (A recitation directed to the

manner in which a claimed apparatus is *intended to be used does not distinguish the claimed*

apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114

and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references*

disclosing generally algorithm/software implemented equivalent embodiments such as that

implemented using the Multilayer Modular Hashing (MMH) algorithm *derivative of the*

associated (RFC) 2401, "Security Architecture for the Internet Protocol" *standard of Ellington et*

al.); "The method of claim 11, wherein

            said authentication comprises

                    application of the *Multilayer* Modular Hashing (MMH) algorithm.".

16.   Claim 13 *additionally recites* the limitation that; "The method of claim 11, wherein

            said authentication comprises

                    application of the Hash-based Message Authentication Code (HMAC) Secure

            Hash Algorithm (SHA)-1.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated authentication/encryption/decryption cryptographic functions

(i.e., col. 5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol", section

4.4.1 "The Security Policy Database", where the authentication/encryption/decryption

cryptographic functions include; AH use of SHA-1/HMAC), clearly encompasses the claimed

limitations as broadly interpreted by the examiner.).

As per claim 20, this claim is the apparatus/system for the method claim 13 above, and is

rejected for the same reasons provided for the claim 13 rejection; "The system of claim *16*,

wherein

> said security processing modules comprise
>
>> a module for performing HMAC authentication.".

17.   Claim 14 *additionally recites* the limitation that; "The method of claim 2, wherein

>   said step (e) comprises

>>   re-encryption of decrypted data from the packet.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated encryption/decryption cryptographic functions (i.e., col.

5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

18.   As per claim 15; this claim is the intended use embodiment of claim 14 above, and is

rejected for the same reasons provided for the claim 14 rejection (A recitation directed to the

manner in which a claimed apparatus is *intended to be used does not distinguish the claimed*

apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114

and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references*

disclosing generally algorithm/software implemented equivalent embodiments such as that

implemented using the Advanced Encryption Standard (AES) *derivative of the associated* (RFC)

2401, "Security Architecture for the Internet Protocol" *standard of Ellington et al.)*; "The method

of claim 14, wherein

    said re-encryption comprises

        encryption performed according to the Advanced Encryption Standard (AES).".

19.   Claim 21 *additionally recites* the limitation that; "The method of claim 3, wherein

    said decryption is performed in

        application layer processing.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54, col.

4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination of a

frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated encryption/decryption cryptographic functions (i.e., col.

5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol" where the

encryption/decryption cryptographic functions include; DES and triple DES), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.).

20.   Claim 22 *additionally recites* the limitation that; "The method of claim 11, wherein

        said authentication is performed in

                application layer processing.".

The teachings of Ellington et al suggest such limitations (ABSTRACT, col. 3,lines 1-54,

col. 4,lines 25-col. 5,line 21, figures 3-11 and associated descriptions, whereas the determination

of a frame as being IP frame or an IPSec frame via the MAC header and protocol field in the IP

header as examined in the data link control layer (i.e., col. 3,lines 17-54) and said IPSec

inherently uses Security association management (SA) and key exchange (i.e., first security

policy) in support of the associated authentication/encryption/decryption cryptographic functions

(i.e., col. 5,lines 13-21, (RFC) 2401, "Security Architecture for the Internet Protocol", section

4.4.1 "The Security Policy Database", where the authentication/encryption/decryption

cryptographic functions include; AH use of SHA-1/HMAC), clearly encompasses the claimed

limitations as broadly interpreted by the examiner.).

Conclusion

21.   Any inquiry concerning this communication or earlier communications from examiner

should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose

unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday

through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization

where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. For more information for

unpublished applications is available through Private PAIR only. For more information about the

PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

Primary Examiner
AU 2131
9/27/05